Privacy Impact Assessment for the

United States Visitor and Immigrant Status Indicator Technology (US-VISIT) Program for the

First Phase of the Initial Operating Capability (IOC) of Interoperability between the U.S. Department of Homeland Security and the U.S. Department of Justice

October 23, 2008

Contact Point
Paul Hasson, Acting Privacy Officer
US-VISIT Program, National Protection and Programs Directorate
(202) 298-5200

Reviewing Official
Hugo Teufel III
Chief Privacy Officer
Department of Homeland Security
(703) 235-0780

Abstract

The United States Visitor and Immigrant Status Indicator Technology (US-VISIT) Program of the Department of Homeland Security (DHS), in cooperation with the Department of Justice (DOJ) Federal Bureau of Investigation (FBI) Criminal Justice Information Services (CJIS) Division, is implementing the first phase of initial operating capability (IOC) of system interoperability (Interoperability) between US-VISIT's Automated Biometric Identification System (IDENT) and CJIS' Integrated Automated Fingerprint Identification System (IAFIS). This capability, which expands upon and improves the method of exchange and sharing of certain biometric and biographic data between IDENT and IAFIS, is intended to increase data sharing between DHS and Federal, State, and local agencies for law enforcement activity relating to the DHS mission. This Privacy Impact Assessment (PIA) describes these uses and sharing of data under the first phase of the Interoperability IOC, as well as the associated privacy risks and measures taken by US-VISIT to mitigate those risks.

Overview

The Automated Biometric Identification System (IDENT) is a Department of Homeland Security (DHS) system, managed by the United States Visitor and Immigrant Status Indicator Technology (US-VISIT) Program, which stores and processes biometric and limited biographic information for DHS national security, law enforcement, immigration, intelligence, and other DHS mission-related functions, and which provides associated testing, training, management reporting, planning and analysis, and other administrative uses. US-VISIT is the system owner of IDENT and, as such, maintains its own collection of information in IDENT as well as data provided by other DHS components and external agencies, including, among others, U.S. Customs and Border Protection (CBP), U.S. Immigration and Customs Enforcement (ICE), U.S. Citizenship and Immigration Services (USCIS), the Transportation Security Administration (TSA), and the U.S. Department of State (DOS). While US-VISIT is the system owner and steward of IDENT, most of the actual data in IDENT is owned and controlled through agreements by the organization(s) that collected the data. Consistent with the IDENT Privacy Impact Assessment[1] (PIA), DHS may share IDENT data (with the consent of the data owner and in accordance with applicable System of Records Notices, policies and regulations) for the purposes of DHS national security, law enforcement, immigration, intelligence, and other DHS mission-related functions as determined by DHS.

Background

[1] See *Privacy Impact Assessment for the Automated Biometric Identification System (IDENT)* (July 31, 2006), located at http://www.dhs.gov/xinfoshare/publications/editorial_0511.shtm#13.

The initial Interoperability pilot effort, known as the interim Data Sharing Model (iDSM), was launched in 2006 and established the platform and necessary processes to support limited data sharing between US-VISIT and the Federal Bureau of Investigation's (FBI) Criminal Justice Information Services (CJIS) Division.[2] The iDSM supports the reciprocal sharing of a specific, limited set of IDENT data and CJIS' Integrated Automated Fingerprint Identification System (IAFIS) data for the purpose of biometric matching and subsequent additional information sharing for confirmed matches. CJIS is provided limited access to a subset of IDENT data stored within IAFIS. In particular, the IDENT data shared during iDSM is limited to information on "high-priority" immigration violators provided by DHS/ICE and certain critical visa refusals provided by DOS. CJIS provides US-VISIT with data on certain individuals in the Subject Criminal Master File, namely those who have active wants and warrants and those who have been identified as known or suspected terrorists.

Under the iDSM, CJIS runs a query using fingerprint and biographic data against IDENT data stored within IAFIS. IDENT query results are then returned to CJIS indicating whether a match was found. Any positive-match responses are then forwarded to ICE's Law Enforcement Support Center (LESC) for data verification and interpretation.

First Phase of Interoperability IOC (Initial Operating Capability)

US-VISIT, in cooperation with DOJ FBI CJIS Division, is implementing the first phase of initial operating capability of system interoperability (hereinafter "first phase of Interoperability IOC") between IDENT and CJIS' IAFIS. As a result of this phase of Interoperability IOC, four significant changes will take place:

1) An authorized user will now be able to query IDENT and IAFIS by making a single request through US-VISIT or CJIS, and will receive a single, consolidated response, a process known as Single Search;

2) Through a deployment plan, existing users of either IDENT or IAFIS will be transitioned to the Single Search process, eventually resulting in tens of thousands of new users of IDENT data;

3) IDENT users (i.e., DHS components and DOS) will obtain new data from IAFIS indicating that criminal history for the biometrically-matched individual exists in IAFIS, allowing DHS components to make more informed decisions across the Department;

4) IAFIS users (i.e., Federal, state, local and tribal criminal justice agencies and certain non-criminal justice agencies) will obtain additional data from IDENT, allowing them to identify or verify the identity of those individuals they encounter for defined law enforcement and national security purposes.

Increased Functionality/Single Search

[2] Interim Data Sharing Model (iDSM) PIA http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_usvisit_idsm.pdf

Currently, entities that query both IDENT and IAFIS must submit fingerprints separately to each database in order to determine if relevant information is contained in either or both respectively. Moreover, many potential users of IDENT are unable to query that database because they do not have connectivity to DHS. The first phase of Interoperability IOC resolves these limitations. Subject to an incremental deployment plan, any existing user of IDENT or IAFIS will be able to submit one set of fingerprints to either US-VISIT or CJIS and that set of fingerprints will be queried against both databases without additional input from the user. Additionally, as users are added incrementally to Interoperability, entities that could not previously access IDENT will be able to do so through the existing connection from IAFIS to IDENT. Therefore, a single transaction will be launched through a single interface, resulting in a "Single Search" request.

Increased User Base

The first phase of the Interoperability IOC will permit access to IDENT and IAFIS to a greater number of authorized users. In the end state, tens of thousands of additional users of IDENT will be incorporated, although access will occur incrementally as resources permit. Initially, the deployment of Interoperability to new users will focus on law enforcement agencies, particularly those at the state and local levels. Other criminal justice and non-criminal justice users will be added when possible. All new users must qualify as an Authorized User and have an Authorized Use, as defined in the Interoperability memorandum of understanding[3] (MOU). Non-criminal justice users in particular must be reviewed and approved by DHS on a case-by-case basis. DHS must determine whether an appropriate use, in accordance with DHS mission purposes, exists, prior to allowing a query of IDENT for these users.

Expanded CJIS Sharing with USVISIT

CJIS will share an indicator of criminal history to assist DHS stakeholders in determining eligibility for benefits, adjudication of visa application and determining admissibility, among other mission-related uses. US-VISIT will receive notification from CJIS that a criminal history record for the biometrically-matched individual exists in IAFIS. US-VISIT will use this notification to create a new encounter in IDENT that provides a pointer to that criminal record for use by IDENT users in future encounters with that individual.

Expanded DHS Information Sharing with CJIS

[3] DHS and DOJ, along with DOS, signed a MOU that under specified circumstances allows data collected by IAFIS users to be stored in IDENT and used for DHS mission-related purposes.

Under iDSM, users were able to access only a small subset of IDENT data. This data was comprised of individuals for whom notification should have been provided to ICE if the individual was encountered by those CJIS users with access to iDSM.

The first phase of Interoperability IOC is different from the iDSM functionality as it will increase the amount of data currently shared between US-VISIT and CJIS by allowing a search of IDENT consisting of all IDENT data except those excluded under the Interoperability MOU or due to routine-use limitations in an applicable System of Records Notice (SORN). Specifically, US-VISIT will share basic biographic data elements with criminal justice and certain non-criminal justice users for identity verification purposes. For example, in Texas, the Harris County Sheriff's Department would now be able to use the biographic data from IDENT to determine if an individual arrested locally has previously identified themselves to a DHS component using a different name or date of birth, which may launch additional investigative efforts. Another example, that of a non-criminal justice entity, is the Office of Personnel Management, which would review the biographic data for inconsistencies in a Federal employment application information as part of the process of performing background investigations.

Section 1.0 Characterization of the Information

The following questions are intended to define the scope of the information requested and/or collected as well as reasons for its collection as part of the program, system, rule, or technology being developed.

1.1 What information is collected, used, disseminated, or maintained in the system?

As discussed in the IDENT PIA published on July 31, 2006, IDENT collects biometric, biographic, and encounter-related data for operations/production, testing, and training environments. Biometric data includes, but is not limited to, fingerprints and photographs. Biographic data includes, but is not limited to, name, date of birth, nationality, and other personal descriptive data. The encounter data provides the context of the interaction with an individual including, but not limited to, location, document numbers, and/or reason for collecting information. Test data may be real or simulated biometric, biographic, or encounter-related data.

While Interoperability is primarily an activity that facilitates the sharing of previously collected data stored in IDENT, it also serves as a limited data collection activity.

Under the first phase of the Interoperability IOC, for any individual for whom a record is retained in IDENT, and who is also discovered to have a record in IAFIS, a new encounter will be created in IDENT immediately following a biometric match. The new encounter will include a pointer—an indicator within the IDENT record to "point" a user to another information source but which will not contain contextual criminal history information. The original collection of criminal information found in IAFIS, which can be obtained using the pointer, is the result of law enforcement activities conducted by Federal, State, local, and tribal criminal justice agencies. A new encounter based on law enforcement records may only be created in IDENT if an IDENT record already exists—eliminating the possibility of holding any criminal history record information without a corresponding immigration and border management encounter. The new encounter will contain limited biographic and biometric elements as follows:

- Full name
- Date of birth
- Place of birth
- Gender
- Race
- 10-fingerprint images
- FBI record identifier
- DHS system record locator

1.2 What are the sources of the information in the system?

The biometric, biographic, and encounter-related information in IDENT is primarily provided by various DHS components (including legacy agency data), DOS, DOJ, and through DOJ CJIS certain information from Federal, state, local, and tribal law enforcement agencies. In particular, DHS provides entry/exit, immigration, enforcement, and credentialing encounters; DOS provides visa encounter data; and DOJ through CJIS provides data relating to criminal history that originates from a Federal, state, local, or tribal law enforcement agency. Additional information provided through CJIS in this phase are basic biographic data (name, date of birth, place of birth, gender, race), fingerprint images, and an FBI number. Other Federal, foreign, and international agencies provide information collected through select law enforcement and intelligence activities for maintenance in IDENT.

1.3 Why is the information being collected, used, disseminated, or maintained?

The two-fold purpose of Interoperability is to identify the existence of criminal history information for immigration and border management adjudication purposes and to facilitate the sharing of information stored in IDENT with an increasing number of authorized criminal and noncriminal justice agencies in order to identify, or verify the identity of, an individual (e.g., upon an arrest or detention or during employment background investigations). All data collected, used, disseminated, and maintained by IDENT is for the purposes of furthering national security, law enforcement, immigration, intelligence, and other DHS mission-related functions.

1.4 How is the information collected?

Most information stored in IDENT is collected directly from an individual through his or her interaction with an immigration and border management, credentialing, or law enforcement process. Such processes include, but are not limited to, applying for a visa, processing at a U.S. port of entry, seeking status as a lawful permanent resident, applying for Federal employment, or being arrested for an immigration violation.

Under the Interoperability IOC, additional criminal history information will be provided by CJIS. That information was originally collected directly from individuals who were fingerprinted by users of IAFIS, who are primarily State and local law enforcement agencies. For example, the Harris County (TX) Sheriff's Office arrests an individual for a crime, those fingerprints are queried against IAFIS and IDENT. If a record already exists in IDENT for that individual, then a new encounter will be created in IDENT indicating that criminal history exists and including a FBI number that can be used to obtain the details, if necessary.

1.5 How will the information be checked for accuracy?

Information collected directly from an individual during an immigration and border management, credentialing, or law enforcement encounter is presumed to be accurate on its face and is specifically checked for accuracy insofar as such a check is part of the process for which the information was originally collected. Information collected from the FBI's IAFIS will be reviewed for accuracy and completeness before or during its use in an immigration and border management or credentialing process by DHS.

With the new Single Search, users will receive a consolidated response from both IDENT and IAFIS. The information returned will include a rap sheet from CJIS and an IDENT Data Response (IDR) from US-VISIT (or nothing from US-VISIT if there is no match). If information on two different individuals is brought up from a single search, it will be clear to the user the source of the information and further investigation may take place to either correct or investigate the reason for mismatching information.

Additionally, US-VISIT also provides individuals with opportunities for correcting inaccurate data through the DHS Traveler Redress Inquiry Program (TRIP), which is described in detail online at www.dhs.gov/trip. More information about TRIP is provided below in section 7.0.

1.6 What specific legal authorities, arrangements, and/or agreements defined the collection of information?

The data maintained in IDENT is collected based on the authority for the programs that originally collected it from individuals. These authorities are described in the PIAs, SORNs, or other materials for each of these programs.

The requirement for interoperability between these systems can be found in various laws and in Congressional appropriations direction, including: the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001; the Enhanced Border Security and Visa Reform Act (Border Security Act) of 2002; and the Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004; as well as in numerous Conference Reports associated with appropriations legislation providing funding to DHS and DOJ since 1999.

DHS and DOJ, along with DOS, signed a MOU that under specified circumstances allows data collected by IAFIS users to be stored in IDENT and used for DHS mission-related purposes.

1.7 Privacy Impact Analysis: Given the amount and type of data collected, discuss the privacy risks identified and how they were mitigated.

A human-factor risk exists for the misuse or misapplication of new data received from IAFIS that is maintained in IDENT under the first phase of the Interoperability IOC. The lack of an IDENT user's understanding and/or a failure of Federal, state, local, and tribal law enforcement agencies to timely and properly update criminal history records may result in an incorrect adjudication based on erroneous information in an individual's IDENT record. For example, law enforcement encounters in which data is entered into IAFIS may be out of date or incomplete because it has not been updated—resulting in a dated or incorrect record, and also resulting in a misinformed adjudication decision that fails to grant a requested benefit within the immigration and border management enterprise.

While the specifics of criminal history data will not be visible in IDENT, when interoperability between IDENT and IAFIS occurs, a pointer back to the IAFIS data will appear if records on an individual exist in both systems. In and of itself, the data may not be derogatory. However, authorized IDENT users unfamiliar or improperly informed on how to read or follow up on a pointer to correctly interpret a criminal history encounter may mistakenly pass judgment on an individual, which may have an undesirable outcome. DHS components with access to

IDENT data have been briefed on the new information and US-VISIT will conduct follow-up regarding operational impacts to these components to ensure proper use of the data.

Another risk of this new information collection from CJIS is that it will not be pre-vetted to determine whether an infraction would make an individual inadmissible or ineligible for a benefit. Once a pointer is appended to the IDENT record, subsequent encounter(s) with an individual whose information is contained in IDENT will likely result in additional inspection or further investigation. This additional action may inconvenience the individual or result in a negative adjudication. This risk is necessary, however, to ensure the thorough and appropriate adjudication of individuals with documented criminal history. Additional inspection of the individual may result in removal of the pointer. Also, DHS is actively vetting records to determine if the pointer should be removed, although this process is not currently conducted in real time. Further, DHS is researching additional automated and manual processes to review IDENT records with an indication of criminal history for possible removal of the pointer.

There are mitigations to the other risks posed by this additional collection of information. The information is limited to the discrete biographic and biometric elements of those individuals having an existing record in IDENT who have also been identified as having criminal history information in IAFIS. By limiting both the depth of the information available in IDENT and the scope of population that may be impacted, the risk of misuse is minimized. Additionally, the IDENT record does not include actual contextual criminal history information, which must still be obtained through NCIC, thus requiring a review process before any adjudication decision is made or action is taken relying on the criminal history information.

Furthermore, if an individual feels the information collected by DHS is inaccurate or incomplete, then redress may be sought and provided through DHS TRIP.

Section 2.0 Uses of the Information

The following questions are intended to delineate clearly the use of information and the accuracy of the data being used.

2.1 Describe all the uses of information.

The Interoperability IOC will expand the accessible number of IDENT data sets, allowing authorized users to conduct searches against all appropriate data maintained in the IDENT database. However, both the data searched and the data returned from a search will be limited by provisions in the Interoperability MOU and data owner restrictions.

As during the iDSM phase of Interoperability, a search by an authorized user will access IDENT data sets that enable the identification of individuals who are deemed high priorities for enforcement action by ICE when they are encountered by law enforcement or in the course of a background investigation. Information returned to an authorized user from a match in one of these data sets will not change from the iDSM.

The additional IDENT data, that will be made available in the first phase of IOC will result in the return of an IDENT Data Response (IDR), which will provide an authorized user with limited biographic information without encounter context, and which is only intended to provide or verify identity. The IDR will include, for up to the five most recent DHS encounters, the following biographic and biometric data elements:

- Full name
- Date of birth
- Place of birth
- Gender
- Photograph
- DHS system record locator

Additionally, new authorized CJIS users—namely Federal, State, local, and tribal law enforcement agencies and certain authorized noncriminal justice agencies meeting IDENT governance standards regarding DHS mission-related use—will be allowed to participate in Interoperability and to submit fingerprints to be searched through the IDENT system. These new users will be incorporated as technical and physical resources permit, which will be achieved through a deployment plan currently in review by all parties, and which is anticipated to begin in November 2008.

2.2 What types of tools are used to analyze data and what type of data may be produced?

As with all biometrics submitted to IDENT, biometrics submitted by authorized users through the FBI CJIS Division are processed through the matching system within IDENT for comparison against stored biometrics. The matching system determines: (1) whether the fingerprints can be matched to an existing record, in which case a new encounter is created as part of that record, or (2) cannot be matched to an existing record, in which case no information is retained in IDENT.

2.3 If the system uses commercial or publicly available data please explain why and how it is used.

The First Phase of Interoperability IOC will not use commercial or publicly available data.

2.4 Privacy Impact Analysis: Describe any types of controls that may be in place to ensure that information is handled in accordance with the above described uses.

The MOU, which was signed on August 4, 2008, contains provisions delineating authorized users and authorized uses, and limits the use of data shared between the Parties or with third parties. Additionally, use is controlled in part by the nature of the record against which a match is made. A match in IDENT data sets deemed to be high priority for enforcement action by ICE will provide highly limited information, not including biographic identifiers, which must be verified and interpreted by ICE's LESC in order to make the originally provided data actionable. A match in the remaining data sets in IDENT will result in a return of limited biographic information without encounter context, which is intended only to provide a verification of identity. Furthermore, if an individual feels the information collected by DHS is inaccurate or incomplete, then redress may be sought and provided through DHS TRIP.

Section 3.0 Retention

The following questions are intended to outline how long information will be retained after the initial collection of data.

3.1 What information is retained?

Under the first phase of the Interoperability IOC the following newly available information will be retained in IDENT when a new encounter is established due to the existence of a criminal history record in IAFIS:

- Full name
- Date of birth
- Place of birth
- Gender
- Race
- 10-fingerprint images
- FBI record identifier
- DHS system record locator

3.2 How long is information retained?

IDENT records will be retained for 75 years, provided that any applicable statutes of limitations have expired for all criminal violations. The provision of IDENT data for storage by FBI/CJIS is contingent upon data continuing to be held in IDENT. Therefore, the retention period for the IDENT data stored by FBI/CJIS will comply with the same restrictions for IDENT.

3.3 Has the retention schedule been approved by the component records officer and the National Archives and Records Administration?

A revised retention schedule for IDENT is currently pending approval by the National Archives and Records Administration (NARA).

3.4 Privacy Impact Analysis: Please discuss the risks associated with the length of time data is retained and how those risks are mitigated.

There is no change to reasons governing the retention period for data in IDENT based on the new collection of data under the first phase of the Interoperability IOC. IDENT data is retained for the minimum period necessary to carry out DHS's national security, law enforcement, immigration, intelligence, and other mission-related functions.

Section 4.0 Internal Sharing and Disclosure

The following questions are intended to define the scope of sharing within DHS.

4.1 With which internal organization(s) is the information shared, what information is shared and for what purpose?

As IDENT is the primary DHS-wide repository for biometrics, data maintained in IDENT may be shared throughout DHS for mission-related purposes. This sharing is often guided by information sharing and access agreements and/or are outlined in operationally specific PIAs and SORNs that are prepared by the component.

In addition to the information described in the IDENT PIA, under the first phase of the Interoperability IOC information obtained from IAFIS will be stored in IDENT and made available to users of IDENT. For those individuals whose fingerprints are submitted by authorized users and which result in a match in IDENT, the newly available information will be in the form of a new encounter and will consist of limited biographic information and fingerprints. These encounters will not, however, contain criminal histories, which will continue to be retrieved through separate existing access to a database unrelated to the Interoperability project. DHS stakeholders may then use this new information, made known to them through this first phase of the Interoperability IOC, to make better informed and timelier decisions about admissibility and benefit eligibility for covered individuals.

4.2 How is the information transmitted or disclosed?

Data from IDENT may be disclosed through DHS components by authorized use of an IDENT interface known as the Secondary Inspections Tool (SIT). Available search parameters of the SIT only allow for one record at a time to be searched and displayed for any particular user. Alternatively, data from IDENT may be transmitted between IDENT and other systems on the DHS core network, an unclassified, secured wide-area network. Other types of transmission or disclosure may be required in some circumstances to meet the mission needs of a DHS component.

4.3 Privacy Impact Analysis: Considering the extent of internal information sharing, discuss the privacy risks associated with the sharing and how they were mitigated.

While additional information will be available to DHS stakeholders, this information is an indication of criminal history and could be obtained by these stakeholders through other means. In addition, all DHS components will be required to access IDENT data through the existing interface or other standard processes, all of which incorporate rules and responsibilities regarding proper use of the information. Further, as the actual criminal history will not be maintained in IDENT, there is no risk that it could be maintained in such a way as to call into question its accuracy, timeliness, or completeness.

Section 5.0 External Sharing and Disclosure

The following questions are intended to define the content, scope, and authority for information sharing external to DHS, which includes Federal, State, and local government, and the private sector.

5.1 With which external organization(s) is the information shared, what information is shared, and for what purpose?

Under the first phase of the Interoperability IOC, expanded information sharing will be conducted with authorized FBI CJIS Division stakeholders, including State and local law enforcement agencies and certain authorized noncriminal justice agencies as allowed by the MOU, unless the sharing of specific information maintained in IDENT is not allowed by the SORN for the original data collection. If a search of IDENT results in the identification of an individual who is deemed a high priority for enforcement action by ICE, only highly limited information will be shared and it will not include biographic data. For this information to be actionable by an authorized user, it must be verified and interpreted by ICE’s LESC. If a search of IDENT results in a match in the remaining data sets in IDENT, the information returned to the authorized user will consist of limited biographic information without an encounter context, which is intended only to provide or verify identity.

This process of data sharing will allow the FBI CJIS Division’s criminal and noncriminal justice stakeholders to improve identification or to verify identity, as well as to determine if an apprehended individual is an alien who is subject to federal enforcement action.

Through the first phase of the Interoperability IOC, the number of authorized external users will expand in accordance with a series of site selection/deployment plans launching shortly after publication of this PIA. These newly authorized Interoperability users, all of which are current criminal and noncriminal justice users of the IAFIS system, will be granted limited access to appropriate data maintained by IDENT. Currently, IDENT data is shared through the iDSM with authorized users limited to the Boston Police Department, Dallas and Harris Counties’ sheriff’s offices operating through the Texas Department of Public Safety, and four county sheriff’s offices operating through the North Carolina Department of Justice for law enforcement purposes; OPM for background security investigations for individuals seeking Federal employment; and DOD for national security purposes.

The first phase of the Interoperability IOC will pick up where iDSM leaves off, to potentially include approximately 84,000 CJIS users in the end state. Initially, the users brought onto Interoperability will be criminal justice users at the Federal, state, local and tribal levels. Non-criminal justice users are expected to be added one by one as DHS reviews requests for their inclusion. A number of criteria have been developed to assist in determining whether the proposed Interoperability user has an appropriate DHS mission-related use. For example, a Federal agency that vets individuals requesting access to nuclear power facilities would have a DHS mission-related use (national security), but a Federal agency that vets individuals seeking employment at a bank would not have a DHS mission-related use.

5.2 Is the sharing of personally identifiable information outside the Department compatible with the original collection? If so, is it covered by an appropriate routine use in a SORN? If so, please describe. If not, please describe under what legal mechanism the program or system is allowed to share the personally identifiable information outside of DHS.

The sharing of personally identifiable information outside the Department is compatible with the purposes for which it was originally collected, as explained in the IDENT SORN, and is covered under the routine uses of that SORN, particularly Routine Uses A and B. All or a portion of the data contained in IDENT records may be disclosed as a routine use covered under

5 U.S.C. 552a (b) (3), where it is acceptable to disclose IDENT information outside of DHS to appropriate Federal, State, local, tribal, foreign, or international agencies for the specific purposes of administering or enforcing the law, national security, immigration, or intelligence, or carrying out DHS mission-related functions as determined by DHS (Routine Use A). Also, all or a portion of the data contained in IDENT records may be disclosed outside DHS as a routine use covered under 5 U.S.C. 552a (b) (3), where it is acceptable to disclose IDENT information outside of DHS as part of a background check or security screening in connection with hiring, retention, performance of a job function, or issuance of a license or credential (Routine Use B).

5.3 How is the information shared outside the Department and what security measures safeguard its transmission?

IDENT data is generally transmitted or disclosed to external organizations in one of three ways:

1. Direct limited access to IDENT where personnel of these organizations are co-located with DHS personnel with access to the system;
2. Limited direct connections to other systems where data may be transmitted directly between IDENT and those other systems; and
3. Secure transfer on portable media when there is no direct connection between systems.

All shared information will be sent between the CJIS network and the Immigration and Customs Enforcement Network (ICENET). The FBI CJIS Division will share DHS information with its stakeholders via its own existing secured systems.

5.4 Privacy Impact Analysis: Given the external sharing, explain the privacy risks identified and describe how they were mitigated.

There is a risk that users who are not yet authorized to request/obtain information will gain access and a related risk of data being transmitted outside of US-VISIT prior to authorization being granted. Under the first phase of the Interoperability IOC, information is being made available to a growing number of Federal, State, and local law enforcement agencies. The potential for unauthorized use or misinterpretation of IDENT data is mitigated by controlling the universe of criminal and noncriminal justice agencies participating in Interoperability, limiting the amount of data shared based on specific circumstances described in the MOU, basic education on the use of DHS data and follow up, as appropriate, on the use of the data with the end users. The MOU requires proper user and use authorization and requires Parties to ensure that such an authorization exists before a search is initiated. It is the responsibility of all Parties to the MOU to require proper authorization for all users and to verify that such authorization exists before a search request is entered into the other party's system.

In addition, to ensure that any biometrically matched data from "high priority" data sets are properly verified and interpreted prior to any action being taken by an authorized user, such data is reviewed by the LESC. A match in the remaining data sets in IDENT will result in the return of an IDR, which provides limited biographic information without encounter context, and which is intended only to provide a verification of identity. Additionally, a filter is under development to prevent the sharing of data maintained in IDENT for which there is no routine use for sharing data for law enforcement purposes under the SORN governing the original collection of information.

In addition, a MOU between and among DHS, DOJ, and DOS, as well as a number of jointly developed system documents, reflect the scope and specific controls in the first phase of the Interoperability IOC, including the protection and use of the data being shared.

Section 6.0 Notice

The following questions are directed at notice to the individual of the scope of information collected, the right to consent to uses of said information, and the right to decline to provide information.

6.1 Was notice provided to the individual prior to collection of information?

Notice is provided by means of the publication of the IDENT PIA, the iDSM PIA, and this PIA on the DHS Web site and extracts of each in the Federal Register, as well as publication of the IDENT SORN on the DHS Web site and in the Federal Register.

6.2 Do individuals have the opportunity and/or right to decline to provide information?

The data maintained in IDENT that is shared with authorized users has previously been collected from DHS components and DOS. Individuals have the opportunity or right to decline to provide the data. However, in doing so they waive the opportunity to become eligible for the benefits for which they are applying.

6.3 Do individuals have the right to consent to particular uses of the information? If so, how does the individual exercise the right?

The collected data, whether from DHS, DOS, or DOJ sources, is used only for the purposes of national security, law enforcement, immigration, intelligence, and other DHS-related mission purposes, as defined by DHS and as described in the IDENT SORN. Once they have provided the information, individuals have no opportunity to consent to or refuse the use of this data for any of these purposes. Individuals seeking Federal employment requiring a background security investigation by OPM provide specific consent for the search of all necessary records.

6.4 Privacy Impact Analysis: Describe how notice is provided to individuals, and how the risks associated with individuals being unaware of the collection are mitigated.

Notice is provided by publication of this PIA on the DHS Privacy Office Web site and by publication of an abstract of this PIA in the Federal Register. The data shared under the first phase of the Interoperability IOC has been previously collected with the knowledge, and generally the consent, of individuals for the purposes of national security, law enforcement, immigration, intelligence, and other DHS-related missions. In most cases, individuals do not have the right or opportunity to decline to share this data or to consent to particular uses. However, through its Privacy Officer, US-VISIT, as the steward of all data maintained in IDENT, ensures that the privacy of all affected individuals is respected and responds to individual concerns raised about the collection and accuracy of the data.

Section 7.0 Access, Redress and Correction

The following questions are directed at an individual's ability to ensure the accuracy of the information collected about them.

7.1 What are the procedures that allow individuals to gain access to their information?

There are no changes to an individual's ability to access his or her information contained in IDENT as discussed in the IDENT PIA. An individual should consult the DHS FOIA website for complete information on how to file a FOIA request, which may be submitted to: FOIA, The Privacy Office, U.S. Department of Homeland Security, 245 Murray Drive SW, STOP-0550, Washington, DC 20528-0550. For more information regarding redress or access to individual information in IAFIS and maintained by CJIS, an individual may be required to follow processes as outlined in the DOS/FBI/CJIS PIAs and SORNs. An individual may make a request for his or her own records under either the Freedom of Information Act (FOIA) or the Privacy Act of 1974. However, certain information may be exempt from individual access because access to the data in IDENT could inform the subject of an investigation of an actual or potential criminal, civil, or regulatory violation; or to the existence of the investigation; or could reveal investigative interest on the part of DHS or another agency. Access to the records could permit the individual who is the subject of a record to impede an investigation, tamper with witnesses or evidence, and/or avoid detection or apprehension. However, in other cases, individuals may request access to their data directly through the redress process or other means as provided for in the PIA for each specific program that collects data.

7.2 What are the procedures for correcting inaccurate or erroneous information?

In order to correct inaccurate or erroneous information believed to reside in a DHS system, individuals should submit redress requests through the DHS TRIP Web site, www.dhs.gov/trip, or mail completed documents to DHS Traveler Redress Inquiry Program (TRIP), 601 South 12th Street, TSA-901, Arlington, VA 22202-4220. Once an individual submits a redress form, the individual will receive notification of receipt. DHS TRIP will review the redress form and determine which component/agency will most effectively be able to respond to the submission. When a redress request is related to US-VISIT processing, TRIP will coordinate with US-VISIT. US-VISIT will then review the individual's records and correct the information, if appropriate. DHS TRIP will notify the individual of the resolution of that request.

7.3 How are individuals notified of the procedures for correcting their information?

Individuals are notified by publication of this PIA, through information available on the US-VISIT Web site, and by the possible receipt of information at a port of entry. The redress procedures are established and operated by DHS through TRIP, which may be accessed at www.dhs.gov/trip.

7.4 If no formal redress is provided, what alternatives are available to the individual?

Redress opportunities are provided as described above.

7.5 <u>Privacy Impact Analysis</u>: Please discuss the privacy risks associated with the redress available to individuals and how those risks are mitigated.

Existing processes are in place to provide access to records, and redress to correct erroneous data, maintained in IDENT. Access to records, whether in the form of a FOIA or Privacy Act request, is processed directly by US-VISIT.

For redress, the appropriate data owner (i.e., the agency that performed the original data collection) will be tasked with correcting errors through the DHS TRIP process. In cases where redress requests are received directly, the data will either be corrected by US-VISIT or the requesters will be notified of the appropriate processing agency for the requests. Because data stored in IDENT and shared with FBI/CJIS users is largely for law enforcement purposes, there may be limits on the rights of individuals to access the data. As discussed above and in the IDENT PIA, DHS/US-VISIT has an existing redress process to correct erroneous data stored in its system. However, in most cases the data owner would be required to correct the data, a process that can usually be managed by using the DHS TRIP system.

Section 8.0 Technical Access and Security

The following questions are intended to describe technical safeguards and security measures.

8.1 What procedures are in place to determine which users may access the system and are they documented?

DHS has documented standard operating procedures to determine which users may access the IDENT system. The minimum requirements for access to the IDENT system are documented in the MOU between and among DHS, DOJ, and DOS, and security, technical, and business documentation. In particular, individuals with system access must hold a DHS security clearance, have a need to know the information based on their job responsibilities, and have participated in security and privacy training.

8.2 Will Department contractors have access to the system?

Some contractors may have access to IDENT data. The extent of access will vary based on the need to fulfill the requirements of the contract under appropriate nondisclosure and use limitations, in addition to requirements enumerated in section 8.1 above. US-VISIT ensures that all employees and contractors supporting its systems have limited access based on their roles and that they are trained in the handling of personal information and personally identifiable information (PII).

8.3 Describe what privacy training is provided to users either generally or specifically relevant to the program or system?

As discussed above, users of DHS/US-VISIT systems, specifically the IDENT system, and all employees and contractors supporting its systems, shall have limited access based on their roles and that they are trained in the handling of personal information and PII. Training on the specific systems will be conducted as appropriate. In addition, US-VISIT conducts in-house/in-person Privacy Awareness Training as part of the on-boarding process, which all employees and contractors are required to take within 30 days of entering on duty. Annual refresher training is also provided via CD-ROM/DVD or online for existing employees and contractors.

CJIS provides limited privacy and security training to its authorized users of IDENT data. In addition, authorized CJIS users have experience in handling similar types of data to which they currently have access, and any potential match will be followed up using established procedures to verify and interpret the match by the LESC.

8.4 Has Certification and Accreditation been completed for the system or systems supporting the program?

The US-VISIT security policy, discussed further in section 8.0, requires that the confidentiality and integrity of an individual's personal information be maintained. Accordingly, the IDENT system supporting the first phase of the Interoperability IOC is validated through a Certification and Accreditation process on a regular basis. IDENT was granted authority to operate (ATO) in May 2007; unless reaccredited, that ATO is set to expire in May 2010. The US-VISIT Chief Information Officer determined that this change did not require a new C&A, but the system security plans were updated to address the new functionality and security testing was performed. Moreover, US-VISIT acts as the data steward for those U.S. Government agencies that maintain data on the IDENT system, ensuring that the first phase of the Interoperability IOC complies with privacy requirements governing the collection and use of data stored within and shared with its stakeholders. Accordingly, US-VISIT will seek permission from the U.S. Government agencies that maintain data in the IDENT system to search that data and to coordinate the subsequent sharing of additional information. The data stored by CJIS will be secured in accordance with DOJ and Federal security requirements, including requirements of the Federal Information Security Management Act of 2002.

8.5 What auditing measures and technical safeguards are in place to prevent misuse of data?

Data will be secured by complying with the requirements of the DHS information technology security policy, particularly the DHS 4300A Sensitive System Handbook. This handbook establishes a comprehensive program to provide complete information security, including directives on roles and responsibilities, management policies, operational policies, technical controls, and application rules that are applied to component systems, communications between component systems, and all interfaces between component systems and external systems. The security policy also requires that all users be adequately trained regarding the security of their systems and perform a periodic assessment of physical, technical, and administrative controls to enhance accountability and data integrity. All DHS system users must complete annual security awareness training. External connections must be documented and approved with both parties' signatures in an Interconnection Security Agreement outlining the controls in place to protect the confidentiality, integrity, and availability of information being shared or processed.

8.6 Privacy Impact Analysis: Given the sensitivity and scope of the information collected, as well as any information sharing conducted on the system, what privacy risks were identified and how do the security controls mitigate them?

There are risks that unauthorized users and/or unauthorized uses of the data shared under the Interoperability IOC will occur. However, these risks are substantially mitigated by minimizing data access, limiting the data returned to the requester upon a match, and implementing data verification processes prior to any action being taken by an authorized CJIS user. US-VISIT will maintain an appropriate level of security in accordance with the sensitivity of the data and the requirements of the data owners.

Section 9.0 Technology

The following questions are directed at critically analyzing the selection process for any technologies utilized by the system, including system hardware, RFID, biometrics, and other technology.

9.1 What type of project is the program or system?

The Interoperability IOC is not a stand-alone system; rather, it is a data-collection and data-sharing activity within IDENT.

9.2 What stage of development is the system in and what project development lifecycle was used?

IDENT is a fully developed and deployed system currently in the Operations and Maintenance phase of the System Development Life Cycle. Additional components to the existing IDENT system have been developed and tested for deployment to make the reciprocal sharing of data between IDENT and IAFIS possible.

9.3 Does the project employ technology which may raise privacy concerns? If so please discuss their implementation.

New technology allows the automatic sharing of data. No additional privacy concerns, beyond those already raised above, are noted.

Approval Signature Page

Original signed and on file with the DHS Privacy Office.

Hugo Teufel III
Chief Privacy Officer
Department of Homeland Security